Session Juggler

Elie Bursztein, Chinmay Soman, Dan Boneh, John Michell
Stanford University / Google

About this presentation

Date: 19 April 2012

Conference: WWW 2012

URL: http://ly.tl/p23

Feel free to contact me

if you have any question

Hydrogels are more than meets the eye. They may be useful in making artificial corneas.

Antec

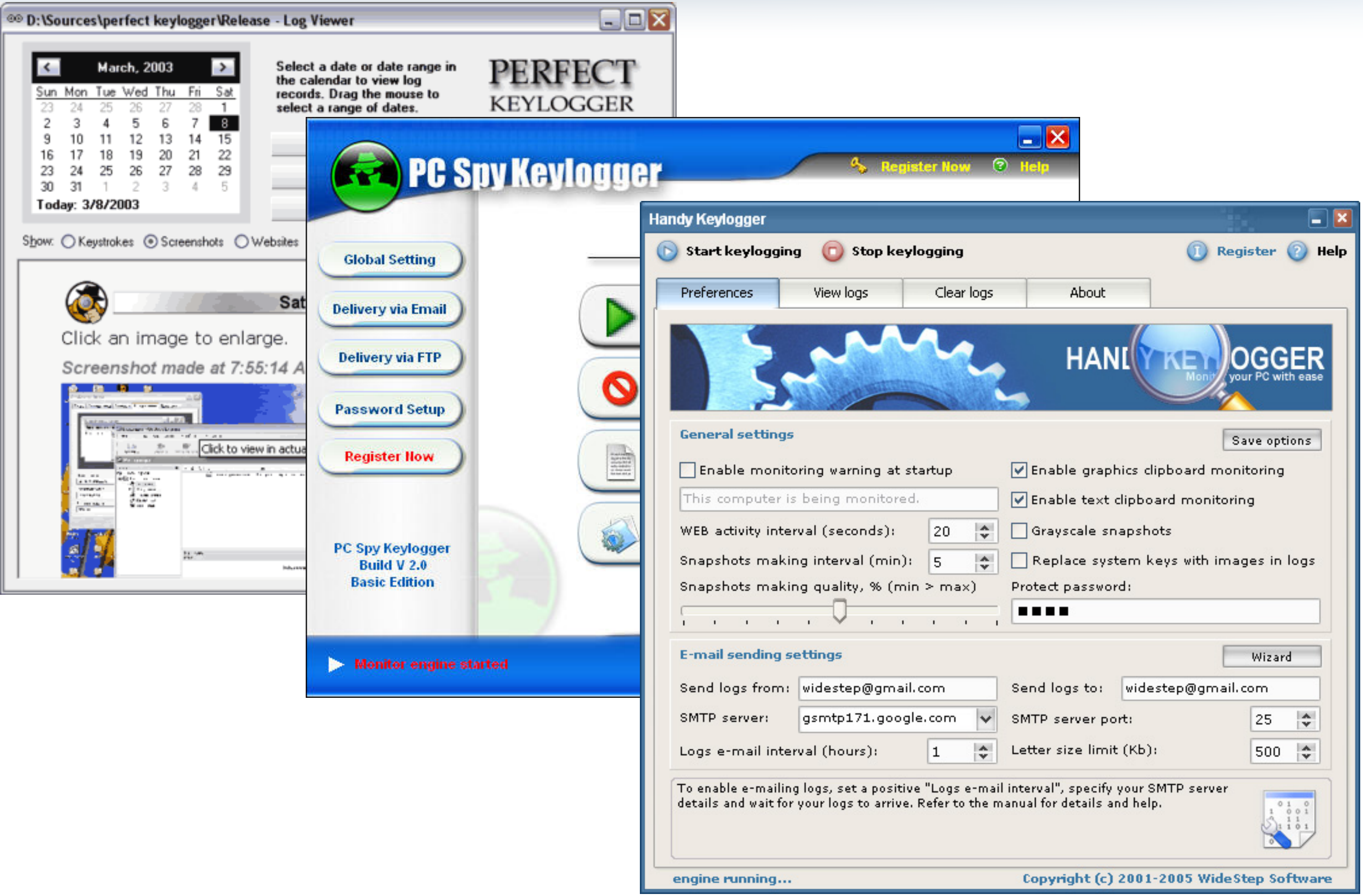
DELL

Afraid of the Dark ?

Hydrogels are more than meets the eye. They may be useful in making artificial corneas.

Afraid of the Dark ?

Looking for something ?



March, 2003						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
23	24	25	26	27	28	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Today: 3/8/2003

Select a date or date range in the calendar to view log records. Drag the mouse to select a range of dates.

Click an image to enlarge.

Screenshot made at 7:55:14 A

PC Spy Keylogger
Build V 2.0
Basic Edition

Monitor engine started

General settings

☐ Enable monitoring warning at startup

This computer is being monitored.

WEB activity interval (seconds): 20

Snapshots making interval (min): 5

Snapshots making quality, % (min > max)

☑ Enable graphics clipboard monitoring

☑ Enable text clipboard monitoring

☐ Grayscale snapshots

☐ Replace system keys with images in logs

Protect password: ■■■■

E-mail sending settings

Send logs from: widestep@gmail.com

Send logs to: widestep@gmail.com

SMTP server: gsmtp171.google.com

SMTP server port: 25

Logs e-mail interval (hours): 1

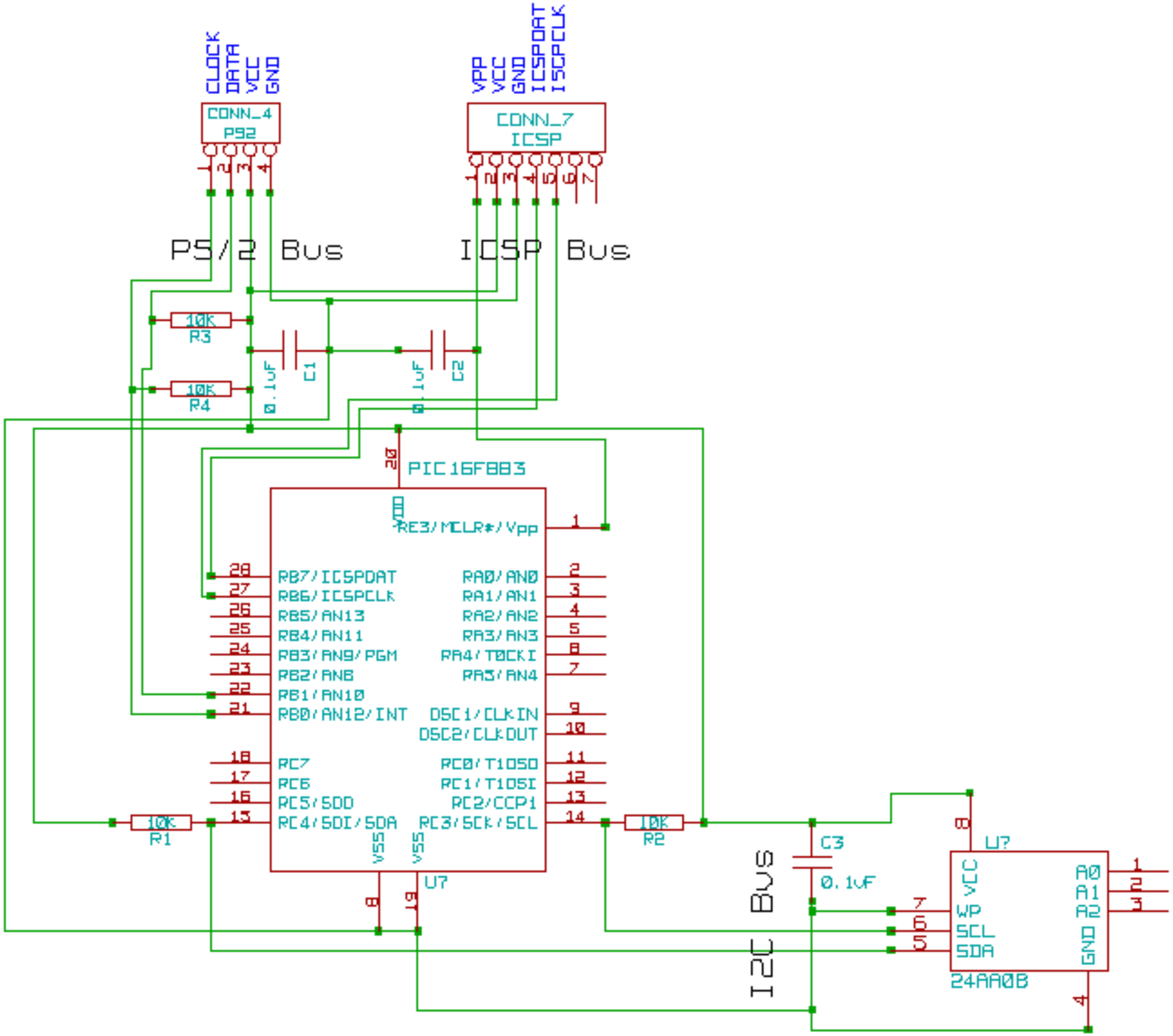
Letter size limit (Kb): 500

To enable e-mailing logs, set a positive "Logs e-mail interval", specify your SMTP server details and wait for your logs to arrive. Refer to the manual for details and help.

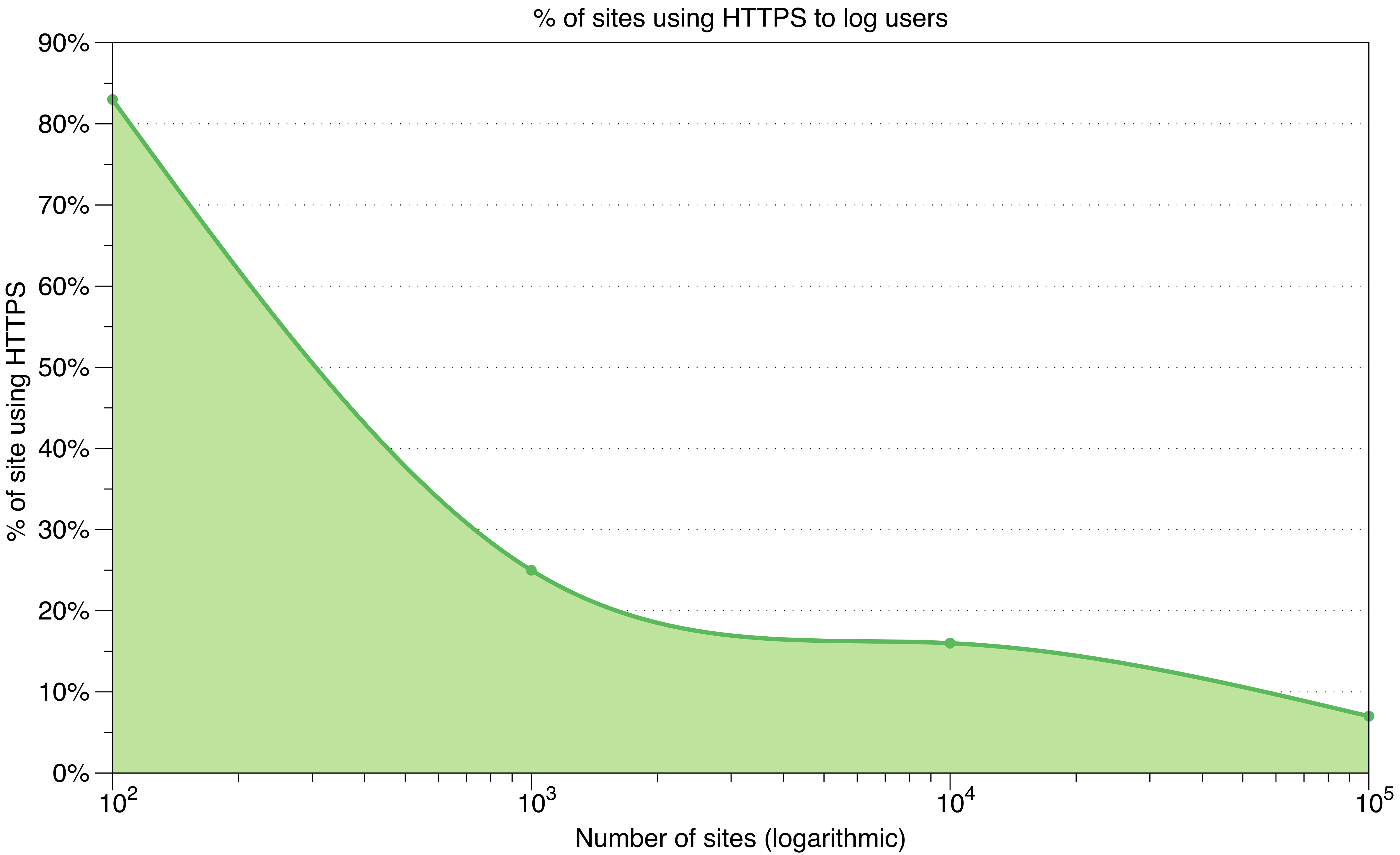
engine running...

Copyright (c) 2001-2005 WideStep Software

Looking for something ?



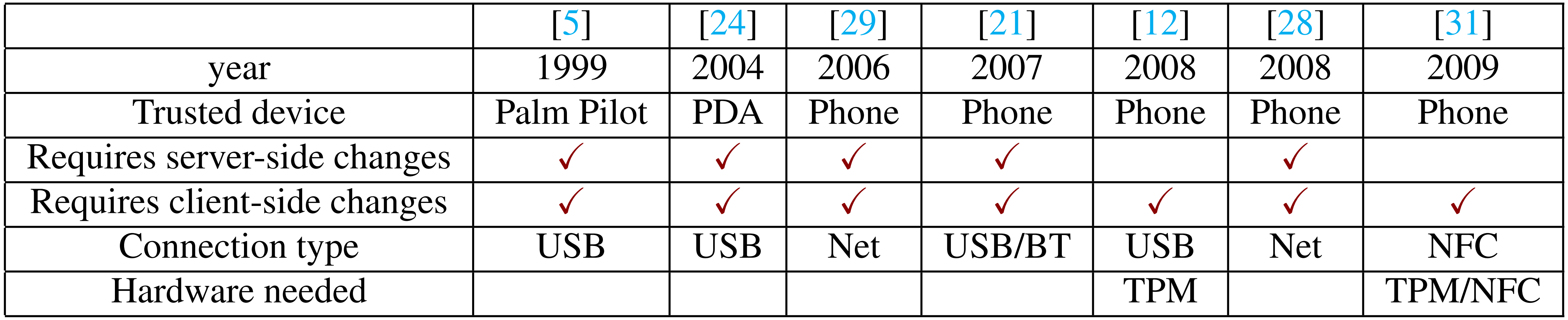
HTTPS adoption



Ephemeral login

- Can’t trust the client at all
- Work for every browser every site
- Use a secure device / secure channel (phone)

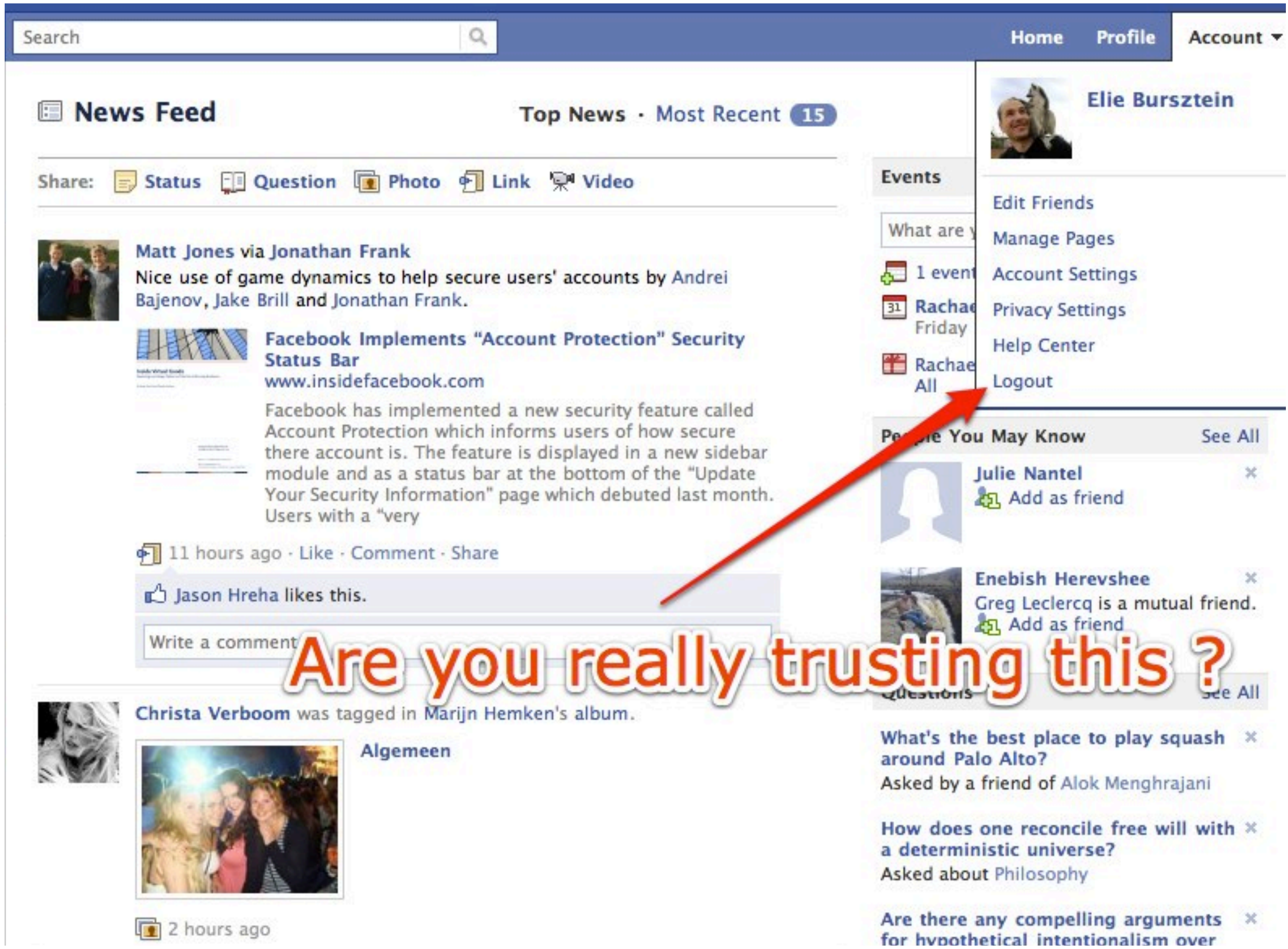
Not that easy



	[5]	[24]	[29]	[21]	[12]	[28]	[31]
year	1999	2004	2006	2007	2008	2008	2009
Trusted device	Palm Pilot	PDA	Phone	Phone	Phone	Phone	Phone
Requires server-side changes	✓	✓	✓	✓		✓	
Requires client-side changes	✓	✓	✓	✓	✓	✓	✓
Connection type	USB	USB	Net	USB/BT	USB	Net	NFC
Hardware needed					TPM		TPM/NFC

Ephemeral login vs OTP

- Site specific
  password list proliferation
- Logout issue
  how to be sure ?



Search

Home Profile Account ▾

News Feed

Top News · Most Recent 15

Share: Status Question Photo Link Video

Matt Jones via Jonathan Frank

Nice use of game dynamics to help secure users' accounts by Andrei Bajenov, Jake Brill and Jonathan Frank.

Facebook Implements "Account Protection" Security Status Bar

www.insidefacebook.com

Facebook has implemented a new security feature called Account Protection which informs users of how secure there account is. The feature is displayed in a new sidebar module and as a status bar at the bottom of the "Update Your Security Information" page which debuted last month. Users with a "very

11 hours ago · Like · Comment · Share

Jason Hreha likes this.

Write a comment...

Christa Verboom was tagged in Marijn Hemken's album.

Algemeen

2 hours ago

Events

What are y

1 event

Rachae
Friday

Rachae
All

Elie Bursztein

Edit Friends

Manage Pages

Account Settings

Privacy Settings

Help Center

Logout

People You May Know See All

Julie Nantel ×
Add as friend

Enebish Herevshee ×
Greg Leclercq is a mutual friend.
Add as friend

Questions See All

What's the best place to play squash around Palo Alto? ×
Asked by a friend of Alok Menghrajani

How does one reconcile free will with a deterministic universe? ×
Asked about Philosophy

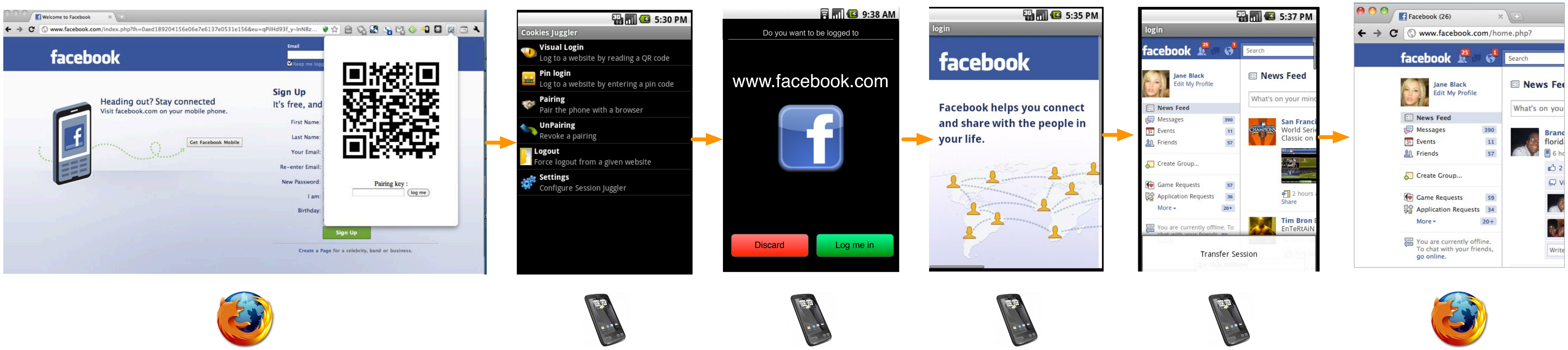
Are there any compelling arguments for hypothetical intentionalism over ×

Are you really trusting this ?

Sometime bad guys make the best good guys

Let’s steal a session (demo)

In case the demo failed :)



Welcome to Facebook

www.facebook.com/index.php?lh=0aed189204156e06e7e6137e0531e156&eu=qPilHd93f_y-InN8z...

Heading out? Stay connected
Visit facebook.com on your mobile phone.

Sign Up
It's free, and

Pairing key :

Cookies Juggler

- Visual Login — Log to a website by reading a QR code
- Pin login — Log to a website by entering a pin code
- Pairing — Pair the phone with a browser
- UnPairing — Revoke a pairing
- Logout — Force logout from a given website
- Settings — Configure Session Juggler

Do you want to be logged to

www.facebook.com

Facebook helps you connect and share with the people in your life.

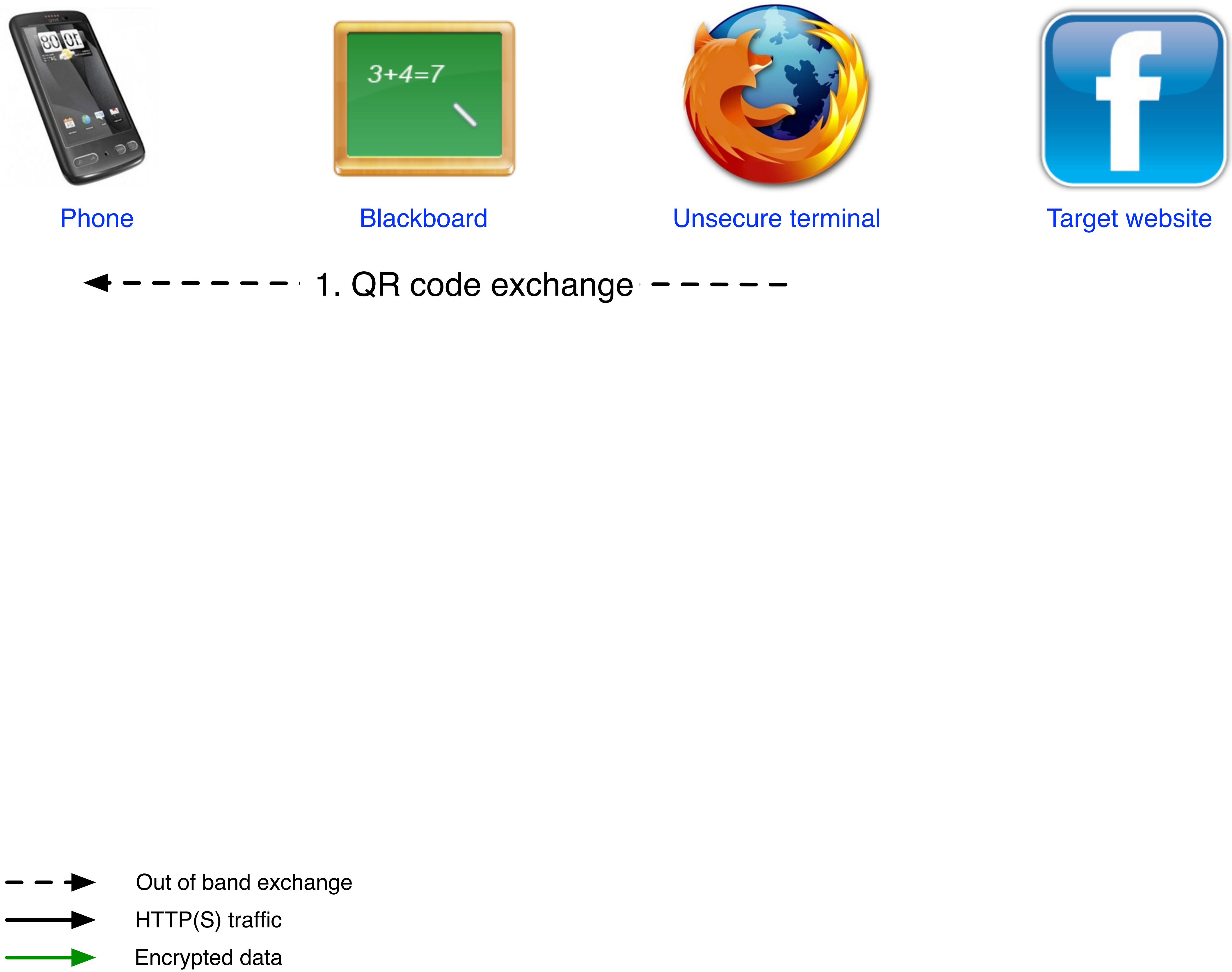
Transfer Session

Facebook (26)

www.facebook.com/home.php?

You are currently offline. To chat with your friends, go online.

Flow view



Phone

Blackboard

Unsecure terminal

Target website

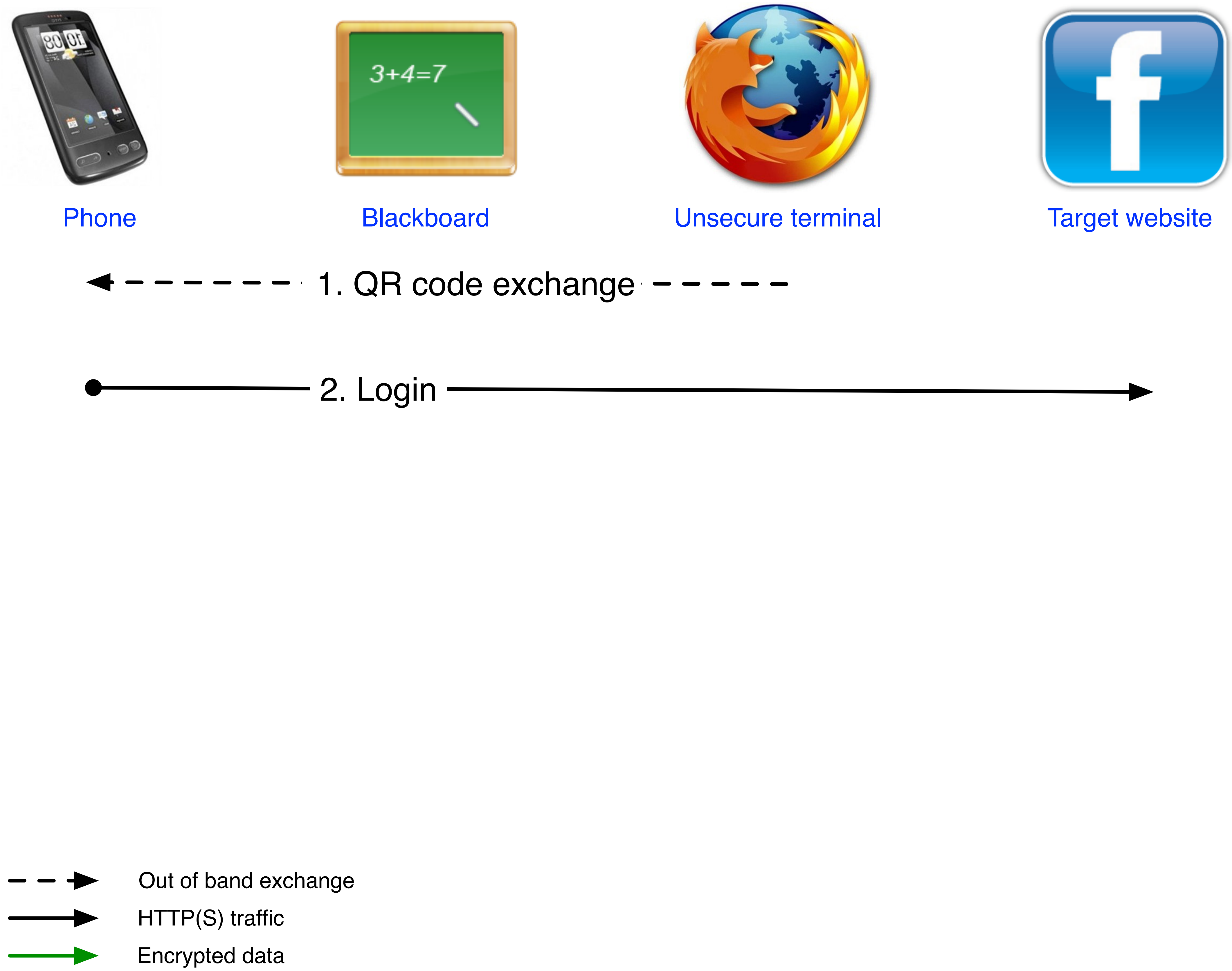
1. QR code exchange

Out of band exchange

HTTP(S) traffic

Encrypted data

Flow view



Phone

Blackboard

Unsecure terminal

Target website

1. QR code exchange

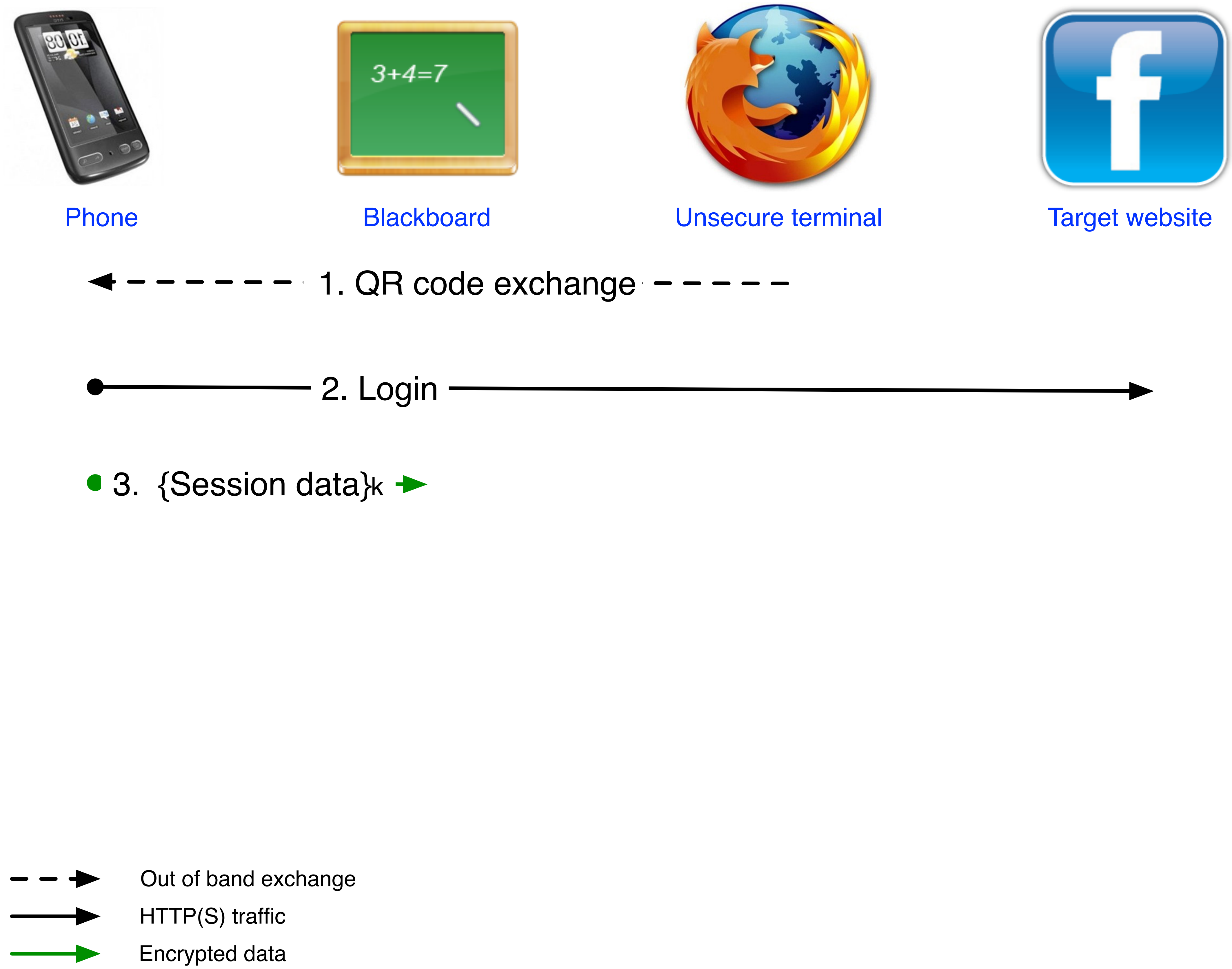
2. Login

Out of band exchange

HTTP(S) traffic

Encrypted data

Flow view



Phone

Blackboard

Unsecure terminal

Target website

1. QR code exchange

2. Login

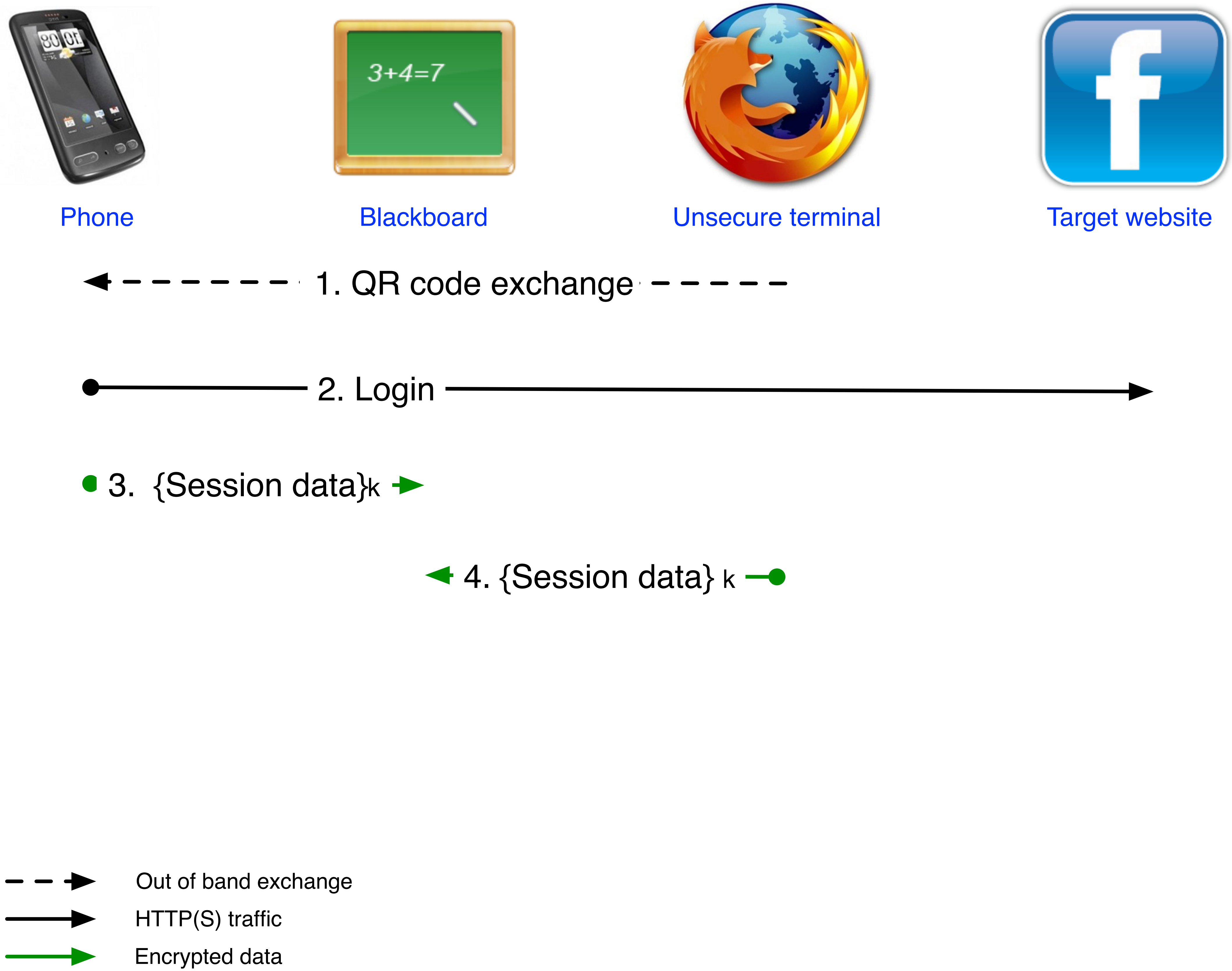
3. $\{\text{Session data}\}_k$

Out of band exchange

HTTP(S) traffic

Encrypted data

Flow view



Phone

Blackboard

Unsecure terminal

Target website

1. QR code exchange

2. Login

3. {Session data}$_k$

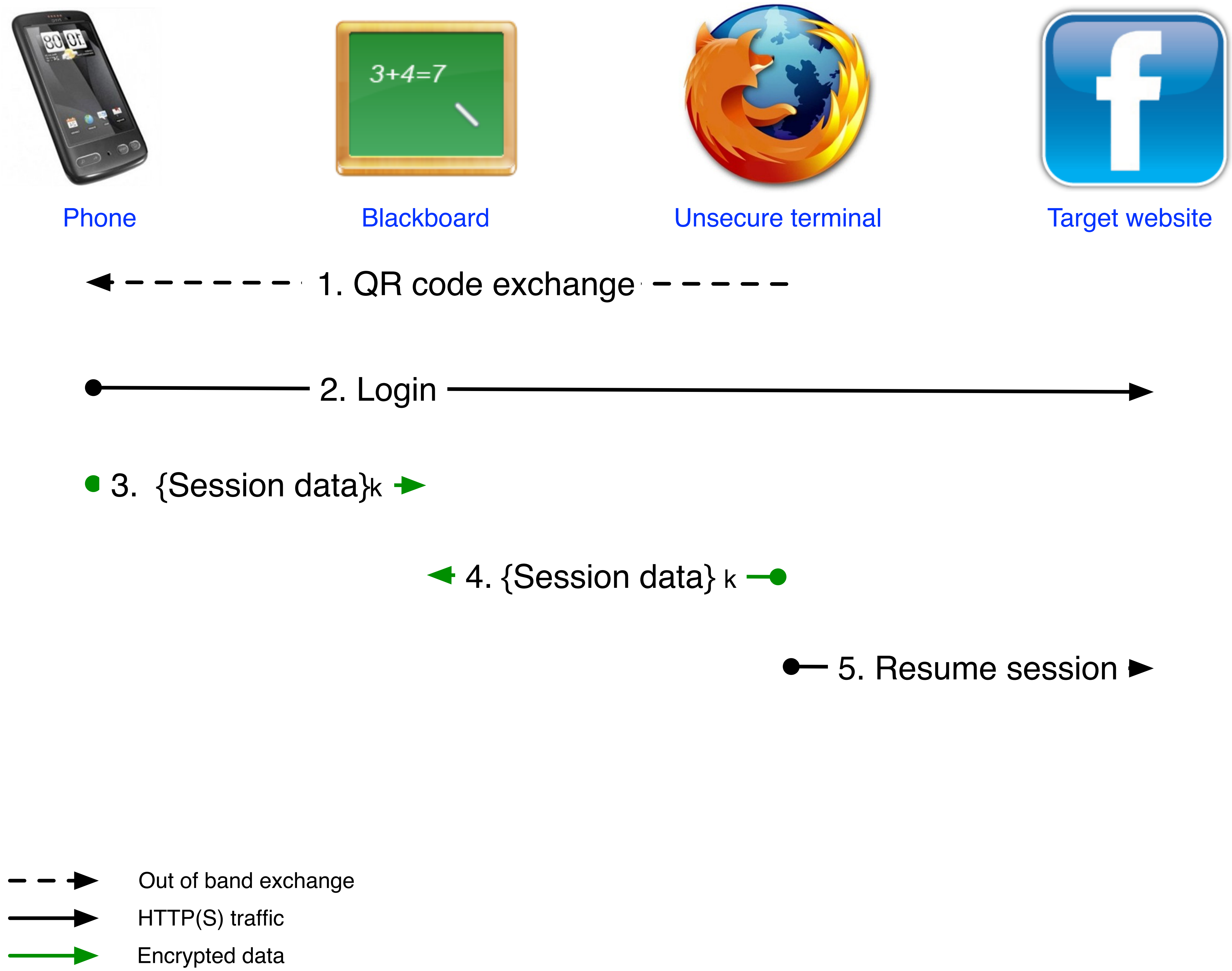
4. {Session data} $_k$

Out of band exchange

HTTP(S) traffic

Encrypted data

Flow view



Phone

Blackboard

Unsecure terminal

Target website

1. QR code exchange

2. Login

3. {Session data}$_k$

4. {Session data} $_k$

5. Resume session

- - ▶ Out of band exchange

—▶ HTTP(S) traffic

—▶ Encrypted data

Hijacking defense

Defense	% of Alexa100
Login over HTTPS	83%
Using secure cookies	52%
Seperating mobile and desktop sessions	6%
Binding session to IP address	8%
Checking local time	1%
Binding session to `user-agent` header	0%
Binding session to local language	0%
Logout over HTTPS	1%

Experimental results

- Works on 98% of the Alexa top 100
- Can be extended to work against arbitrary defense

Conclusion

- Steal http session to provide a temporary login
- No server side or client modification

Thank you

Thank you !

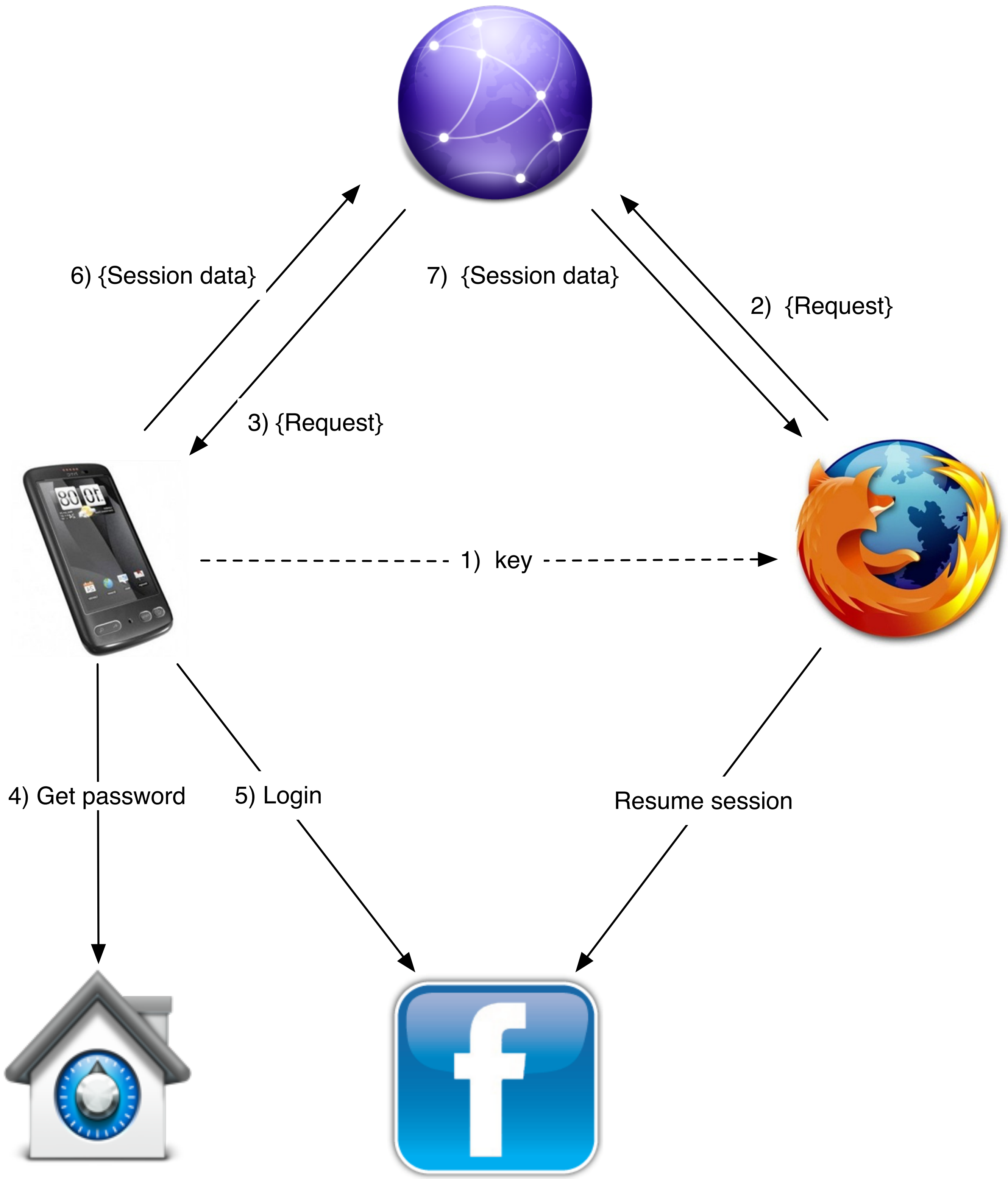
Questions ?

Follow-me !

Google+ / Twitter: @elie

More research: http://elie.im/

Alternative architecture


6) {Session data}
7) {Session data}
2) {Request}
3) {Request}
1) key
4) Get password
5) Login
Resume session